EDINET Electronic Disclosure for Investors' NETwork

書類提出用
端末要件

平成 27 年4月

金融庁　総務企画局　企業開示課

◆Microsoft Corporation のガイドラインに従って画面写真を使用しています。

◆Microsoft、Windows、Windows Vista は、米国 Microsoft Corporation の米国及びその他の国における登録商標又は商標です。

◆Oracle と Java は、Oracle Corporation 及びその子会社、関連会社の米国及びその他の国における登録商標です。文中の社名、商品名等は各社の商標又は登録商標である場合があります。

◆Adobe® product screen shots reprinted with permission from Adobe Systems Incorporated.

◆Adobe、Adobe Photoshop、Adobe Illustrator は、Adobe Systems Incorporated の登録商標又は商標です。

◆その他、記載されている会社名及び製品名は、各社の登録商標又は商標です。

◆本文中では、TM、®、©は省略しています。

◆本文及び添付のデータファイルで題材として使用している個人名、団体名、商品名、ロゴ、連絡先、メールアドレス、場所、出来事等は、全て架空のものです。実在するものとは一切関係ありません。

◆本書に掲載されている内容は、平成 27 年4月現在のもので、予告なく変更される可能性があります。

◆本書で公開している情報の利用については、利用規約（https://submit.edinet-fsa.go.jp/EKW00Z0030.html）を遵守してください。

◆本書に記載の会社名及び製品名について、金融庁はそれらの会社、製品等を推奨するものではありません。

Copyright©金融庁 All Rights Reserved.

1 操作環境について 4

2 事前準備 5

2-1 EDINET 利用時の操作環境 5
2-2 信頼済みサイトへの登録 6
2-3 証明書の設定 8
2-3-1 証明書設定の必要性確認 8
2-3-2 証明書の設定 10
2-4 JRE の設定 11
2-5 電子メールの設定 12
2-6 フィルタリングソフトを導入している場合 12

3 電子署名 13

3-1 電子証明書について 13
3-2 公的個人認証サービスのセットアップ 15
3-2-1 IC カードリーダのドライバセットアップ 16
3-2-2 署名機能クライアントのセットアップ 16
3-2-3 公的個人認証証明書登録ツールのセットアップ 25
3-3 商業登記 31
3-3-1 事前準備 31
3-3-2 証明書の登録 31

本書について

本書は、「**開示書類等提出者のサイト**」を利用するためのコンピュータの事前準備及び必要な設定変更について説明しています。

EDINET を御利用いただくために

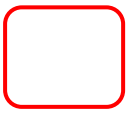
EDINET に開示書類を提出するための前提知識として、一般的な Web ブラウザを使用し、インターネットが御利用いただける方を対象としています。

本書の表記について

本書は次の環境で作成しています。

OS	Microsoft Windows 7 SP1
ソフトウェア	Microsoft Internet Explorer 9 JRE Version8 Update45 Adobe Reader X

本書内に記載している記号は、次のような意味があります。

表示	意味	表示	意味
POINT	操作に関連するポイントについて説明しています。		画面の入力又は選択する項目等を指します。
MEMO	知っておいていただきたいことについて説明しています。		画面で表示された項目を指します。
重要	重要事項について説明しています。必ずお読みください。	《　》	画面の項目名を指します。 例：《EDINET コード》をクリックします。
[　]	画面名を指します。 例：[提出者検索画面]が表示されます。	【　】	キーを押す操作を指します。 例：【F5】キーを押します。

製品名の記載について

本書では、次の略称を使用しています。

名称	略称
Windows 8.1	Windows 8.1 又は Windows
Windows 8	Windows 8 又は Windows
Windows 7	Windows 7 又は Windows
Windows Vista	Windows Vista 又は Windows
Windows Internet Explorer 11	Internet Explorer 11 又は Internet Explorer
Windows Internet Explorer 10	Internet Explorer 10 又は Internet Explorer
Windows Internet Explorer 9	Internet Explorer 9 又は Internet Explorer
Windows Internet Explorer 8	Internet Explorer 8 又は Internet Explorer
Windows Internet Explorer 7	Internet Explorer 7 又は Internet Explorer
Adobe Reader X	Adobe Reader X 又は Adobe Reader

<<EDINET の利用に当たって>>

EDINET を装い、ユーザ ID、パスワード等の個人情報を盗もうとする偽の Web サイトに注意してください。
このような Web サイトに誘導するメールが届いても、リンク先にアクセスしたり、添付ファイルを開いたりしないように注意してください。
EDINET からメールで個人情報を照会することは一切ありません。
なお、ウィルス対策ソフトを最新の状態にするなど、御利用環境のセキュリティ対策をおすすめします。

1 操作環境について

「開示書類等提出者のサイト」を利用する場合の、コンピュータ環境について説明します。

EDINET は、下表に記載のオペレーティングシステム、Web ブラウザ及び「JRE（Java Runtime Environment）」の組合せで動作を確認しています。なお、JRE については JRE8 の最新バージョンを設定することを推奨しています。

JRE の設定手順については、「2-4 JRE の設定」を参照してください。

＜ハードウェア＞

ディスプレイ解像度： 1024×768 以上

＜ソフトウェア＞

オペレーティングシステム	Web ブラウザ				
	Internet Explorer 11 ※1	Internet Explorer 10 ※1	Internet Explorer 9 （32bit）	Internet Explorer 8 （32bit）	Internet Explorer 7
Windows8.1	○	―	―	―	―
Windows8	―	○	―	―	―
Windows7 SP1	○	○	○	○	―
Windows Vista SP2	―	―	○	○	○
JRE	Version8 Update45				

※1 拡張保護モードを無効に設定し、御使用ください。
また、EDINET では、サーバ側で「Internet Explorer9」として互換表示するように設定しています。
ブラウザの互換表示設定をする場合は、「Internet Explorer10」以降のモードを指定しないでください。

※上の表の組合せ以外で EDINET を利用する場合、画面の表示が操作ガイドと一部異なるときがあります。
※EDINET を利用するためには、事前に政府認証基盤（GPKI）のホームページから「アプリケーション認証局2(Root)の自己署名証明書」を入手する必要があります。手順は「2-3-2 証明書の設定」(p.10)を確認してください。
※PDF の書類を閲覧するためのソフトウェア（例：AdobeReader）が必要です。

2　事前準備

EDINET を利用する前に、御利用いただくコンピュータに事前準備が必要です。事前準備の手順について説明します。

2-1　EDINET 利用時の操作環境

EDINET に接続する際に、御利用いただいているコンピュータで、初期設定から変更する箇所について説明します。

1　信頼済みサイトへの登録

↓

2　証明書の設定

↓

3　JRE の設定

2-2 信頼済みサイトへの登録

Internet Explorer を起動し、[**開示書類等提出者のサイト**]を「**信頼済みサイト**」に登録します。「**信頼済みサイト**」には安全であることがわかっている Web サイトの URL を登録しておくことで、登録した Web サイトからのダウンロード及び実行時の警告が表示されず、また、実行時の制限を受けないようにできます。EDINET の［**開示書類等提出者のサイト**］を正しく動作するように利用していただくために、信頼済みサイトへ登録します。

1

Internet Explorer を起動します。

2

メニューバーの《ツール》から《インターネット　オプション》をクリックします。

[**インターネット　オプション**]が表示されます。セキュリティの設定をします。

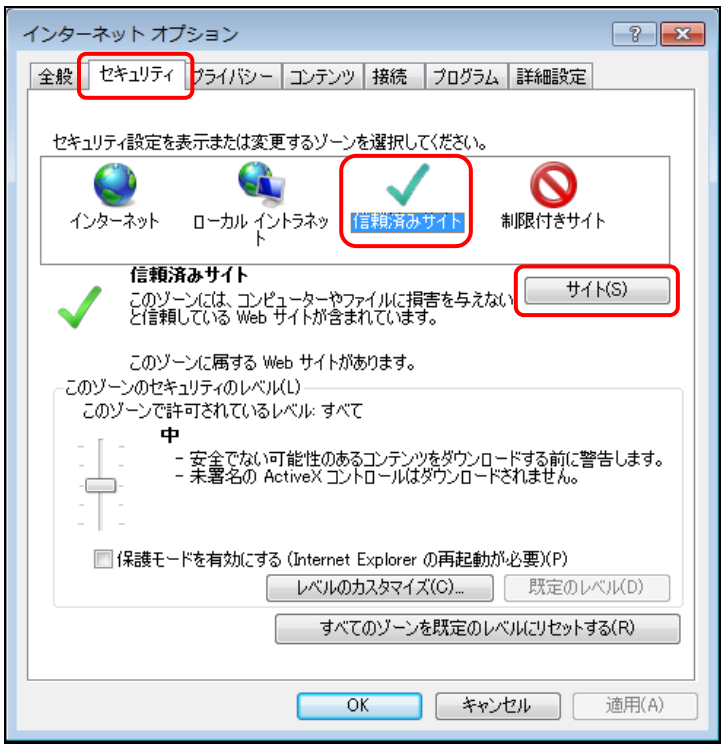
3

《セキュリティ》タブをクリックします。

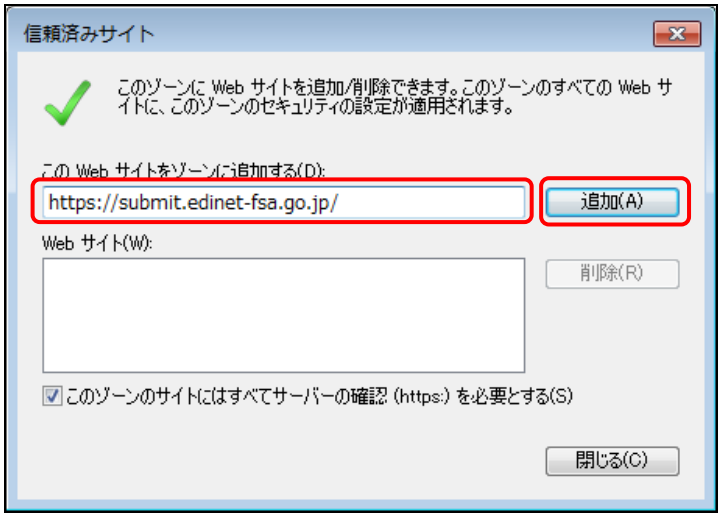
4

（信頼済みサイト）を選択し、

（サイト）をクリックします。



［信頼済みサイト］が表示されます。

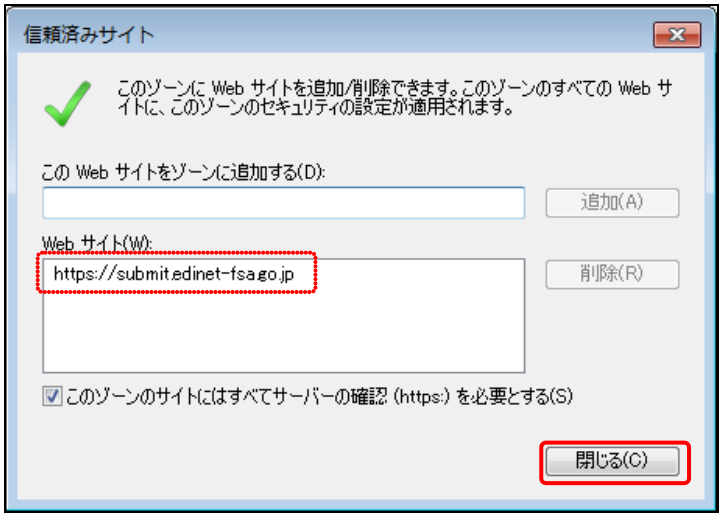


5

《次の Web サイトをゾーンに追加する》に「https://submit.edinet-fsa.go.jp/」と入力します。

6

追加(A)（追加）をクリックします。



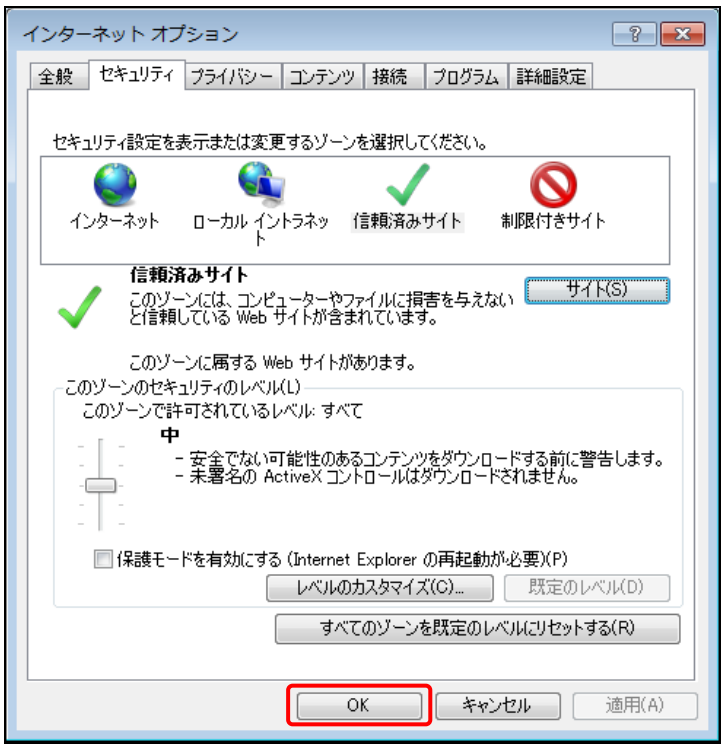
7

《Web サイト》に操作 5 で入力した URL が追加されたことを確認します。

8

閉じる(C)（閉じる）をクリックします。

［インターネット オプション］に戻ります。



9

OK（OK）をクリックします。

2-3 証明書の設定

EDINET を利用するには、「**ルート証明書の更新**」プログラムが有効である必要があります。「**ルート証明書の更新**」プログラムが有効でない方は、政府認証基盤（GPKI）のホームページから「**アプリケーション認証局2(Root)の自己署名証明書**」をダウンロードし、御利用いただくコンピュータに設定してください。

設定の要否については、「**2-3-1　証明書設定の必要性確認**」の操作をし確認します。確認した結果、設定が必要である場合は、「**2-3-2　証明書の設定**」の操作をします。

2-3-1 証明書設定の必要性確認

EDINET の［**開示書類等提出者のサイト**］に接続し、「**アプリケーション認証局2(Root)の自己署名証明書**」を手動で設定する必要があるかを確認します。

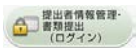
1

Webブラウザを起動し、「開示書類等提出者のサイト」を表示します。

URL　MEMO

http://submit.edinet-fsa.go.jp/ に接続してください。

2

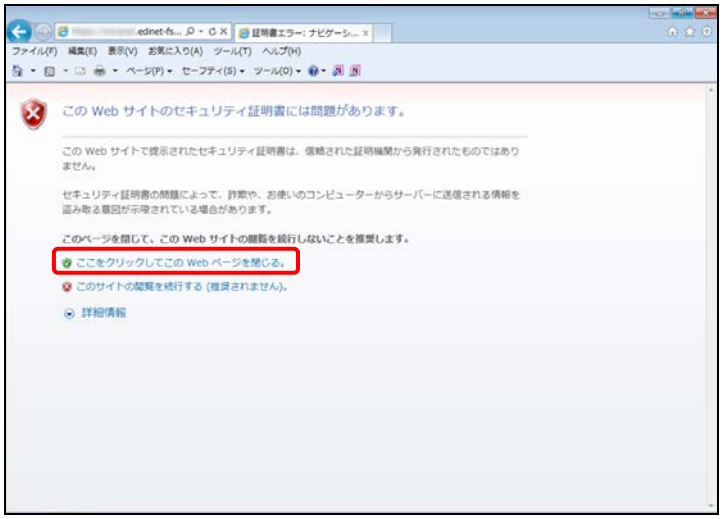


（提出者情報管理・書類提出（ログイン））をクリックします。

3

［セキュリティの警告］が表示される場合は、「2-3-2　証明書の設定」の操作が必要です。

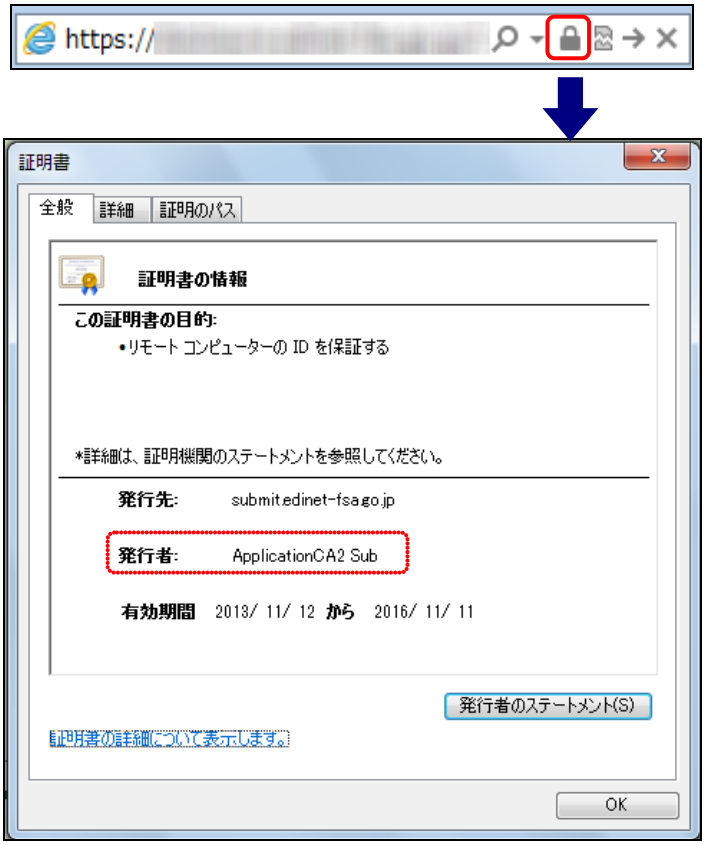
《ここをクリックしてこの Web ページを閉じる》をクリックしてWebブラウザを終了します。



［セキュリティの警告］が
表示されない場合

MEMO

［セキュリティの警告］が表示されない場合は、「2-3-2 証明書の設定」は不要です。Web ブラウザの鍵マークをクリックし、［証明書］を表示します。
《発行者》が「ApplicationCA2 Sub」と表示されることを確認します。



2-3-2 証明書の設定

政府認証基盤（GPKI）のホームページから、「**アプリケーション認証局2(Root)の自己署名証明書**」をダウンロードし、御利用いただくコンピュータに設定します。

1

Web ブラウザを起動します。

2

政府認証基盤（GPKI）のホームページに接続し、「アプリケーション認証局２(Root)の自己署名証明書」をダウンロードし、設定します。
《アプリケーション認証局２》をクリックし、以降の操作は、画面の指示に従ってください。

※本画面は 2013 年 12 月現在のものです。

政府認証基盤（GPKI）のホームページ

MEMO

政府認証基盤（GPKI）のホームページのURL は、https://www.gpki.go.jp/ です。

政府認証基盤（GPKI）のホームページ及び「アプリケーション認証局2(Root)の自己署名証明書」の設定に関する質問は、政府認証基盤（GPKI）のホームページに記載されている、《お問い合わせ》より確認してください。

2-4 JRE の設定

EDINET に書類提出する場合は、事前に Oracle Corporation の「JRE（Java Runtime Environment）」のインストールが必要です。

JRE（Java Runtime Environment）のダウンロードサイト

JRE（Java Runtime Environment）は、次のホームページからダウンロードできます。
※次のホームページは Oracle Corporation で運営されており、金融庁が運営しているものではありません。このアドレスは 2015 年 2 月時点のものです。

http://www.java.com/ja/download/

1

Internet Explorer を起動し、Java のダウンロードサイトを表示します。

2

画面中央にある「無料 Java のダウンロード」ボタンをクリックします。

3

以降の操作は、表示される画面の指示に従ってください。

インストールができない場合　MEMO

インストールができない場合は、自社のシステム管理者に御相談ください。

2-5 電子メールの設定

EDINET では、電子メールを利用して、開示書類等提出者に迅速情報を提供します。御利用のコンピュータから利用が可能な電子メールアドレスを開示書類等提出者ごとに取得してください。電子メールアドレスは、EDINET 利用届出時に入力が必要になります。

2-6 フィルタリングソフトを導入している場合

フィルタリングソフトを導入している場合で、EDINET に書類を提出するときは、次の URL がアクセスできるように設定してください。

<EDINET>

http://submit.edinet-fsa.go.jp/

https://submit.edinet-fsa.go.jp/

https://submit-sorry.edinet-fsa.go.jp/

<政府認証基盤(GPKI)>

https://www.gpki.go.jp/

また、EDINET での書類提出にあたり、JRE(Java Runtime Environment)及び Adobe Reader が必要となります。御利用いただくコンピュータに事前にインストールしておくか、又はそれぞれのダウンロードサイトをアクセスできるように設定してください。

3 電子署名

EDINET に書類提出する際に、電子署名を付与して提出する場合の電子証明書、事前準備について説明します。
※なお、書類提出時の電子署名の付与は任意です。

3-1 電子証明書について

書類提出時に、電子署名を付けて提出する場合は、事前に電子証明書を入手しておく必要があります。

電子証明書は「**政府認証基盤**(GPKI:Government Public Key Infrastructure)」が相互認証した次の民間認証局から発行されている電子証明書を使用してください。

民間認証局の一覧（2015 年 3 月時点）

認証局(会社名)	サービス名	証明書タイプ	動作確認※
電子認証登記所	商業登記認証局		○
日本電子認証株式会社	AOSign サービスに係る認証局 AOSign サービス G2 に係る認証局	IC カード	○
東北インフォメーション・システムズ株式会社	TOiNX 電子入札対応認証サービスに係る認証局	IC カード	○
株式会社帝国データバンク	TDB 電子認証サービス TypeA に係る認証局	IC カード	○
株式会社 NTT ネオメイト	e-Probatio PS2 サービスに係る認証局	IC カード	○
セコムトラストシステムズ株式会社	セコムパスポート for G-ID に係る認証局	ダウンロード、CD-R	
ジャパンネット株式会社	電子入札コアシステム用電子認証サービスに係る認証局 DIACERT サービスに係る認証局 DIACERT-PLUS サービスに係る認証局	IC カード、USB メモリ	

認証局(会社名)	サービス名	証明書タイプ	動作確認※
地方公共団体による公的個人認証サービス	地方公共団体による公的個人認証サービス	IC カード	

※EDINET にて、SHA-256 の電子証明書での動作確認をしている認証局。
　動作確認欄に「○」のない認証局の動作については、各民間認証局に御確認ください。

3-2 公的個人認証サービスのセットアップ

EDINET に書類提出する際に、公的個人認証サービスから発行された署名を付与して提出する場合の事前準備について説明します。

事前に次のドライバ又はアプリケーションソフトウェアを準備します。

事前に準備するもの	説明
□ IC カードリーダドライバ	IC カードリーダをパソコンで使用できるようにするファイルを「**IC カードリーダドライバ**」といいます。パソコンに接続すると、自動セットアップされる場合があります。その場合は不要です。IC カードリーダのホームページ、取扱説明書等で確認し、入手してください。
□ 署名機能クライアント	EDINET の［**開示書類等提出者のサイト**］から入手します。
□ 公的個人認証証明書登録ツール	EDINET の［**開示書類等提出者のサイト**］から入手します。

事前に準備したものを使用し、次の手順でセットアップを進めます。

1 IC カードリーダドライバのセットアップ

電子証明書が登録された IC カードを読み込むためのカードリーダをセットアップします。メーカーによってはカードリーダをパソコンに接続すると、自動セットアップされる場合があります。

2 署名機能クライアントのセットアップ

EDINET の［**開示書類等提出者のサイト**］から署名機能クライアントをダウンロードし、セットアップします。

3 公的個人認証証明書登録ツールのセットアップ

EDINET の［**開示書類等提出者のサイト**］から公的個人認証証明書登録ツールをダウンロードし、セットアップします。

3-2-1 IC カードリーダのドライバセットアップ

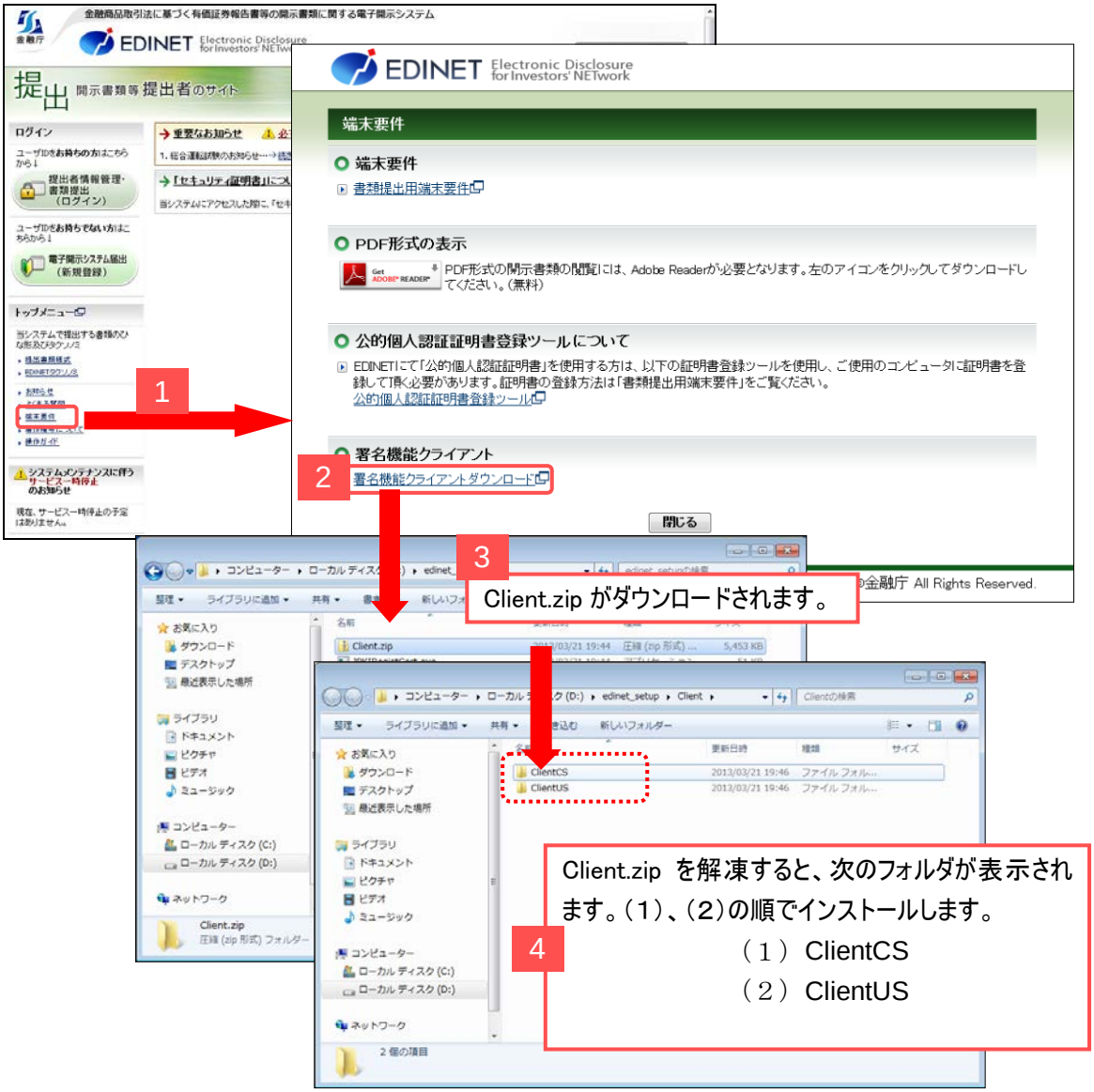
IC カードリーダのドライバをセットアップし、使えるようにします。

使用するパソコンに、IC カードリーダを接続すると自動セットアップされる場合があります。自動セットアップの場合は、しばらく待つとドライバのセットアップが完了します。それ以外の場合は、IC カードリーダを提供しているメーカーのホームページ又は取扱い説明書を確認して、手順に従ってドライバをセットアップしてください。

3-2-2 署名機能クライアントのセットアップ

EDINET からダウンロードした「**署名機能クライアント**」をセットアップします。

「**署名機能クライアント**」は、EDINET の［**開示書類等提出者のサイト**］にある「**トップメニュー**」の「**推奨端末仕様**」から「**署名機能クライアントダウンロード**」をクリックし、ダウンロードします。



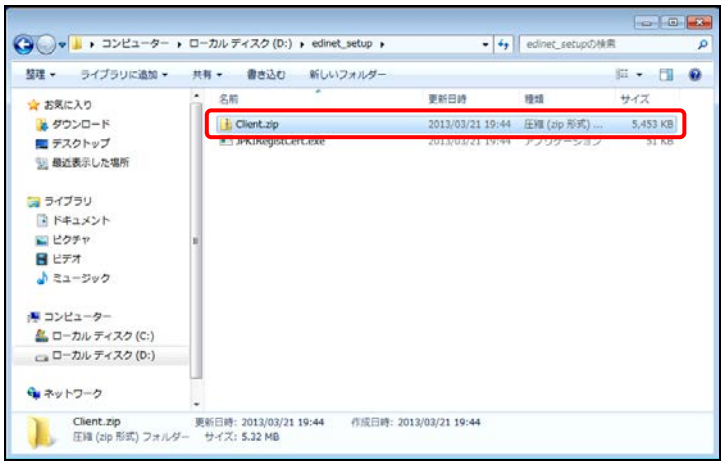
セットアップの手順は次のとおりです。
（1）ダウンロードした「Client.zip」を解凍します。
（2）セットアップファイルの署名を確認します。
（3）署名機能クライアントをセットアップします。

（1） ダウンロードした「Client.zip」の解凍

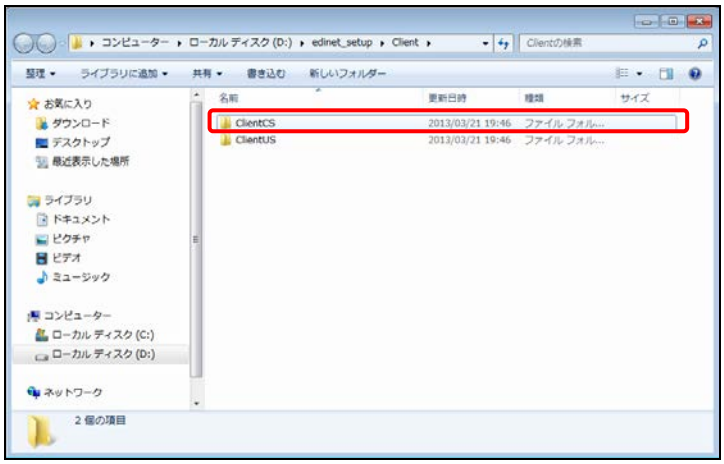
解凍ツールを利用する場合は、ツールの手順に従ってください。

1

ダウンロードした「Client.zip」を解凍します。



「ClientCS」及び「ClientUS」の二つのフォルダが作成されます。



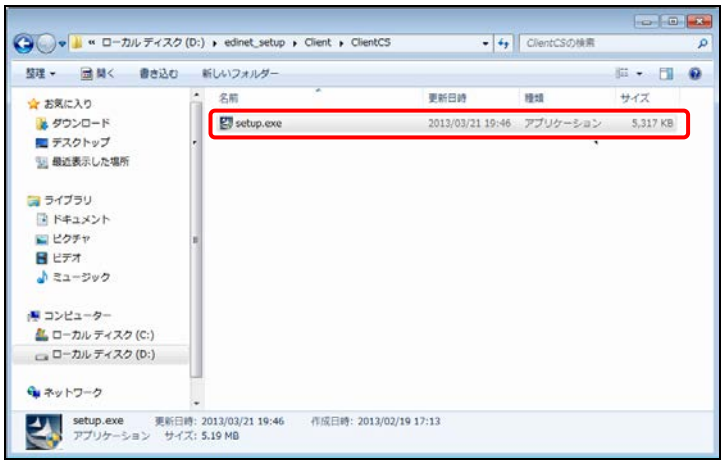
2

「ClientCS」をダブルクリックします。

ClientCS 及び ClientUS POINT

両方をセットアップします。セットアップする順序は「ClientCS」をセットアップ後、「ClientUS」をセットアップします。

「setup.exe」ファイルが表示されます。



拡張子の表示 POINT

Windows の設定が、ファイルの拡張子を表示する設定になっている場合は右の図のように「setup.exe」と表示され、ファイル名の後ろに拡張子「.exe」が表示されます。表示しない設定の場合「setup」と表示されます。

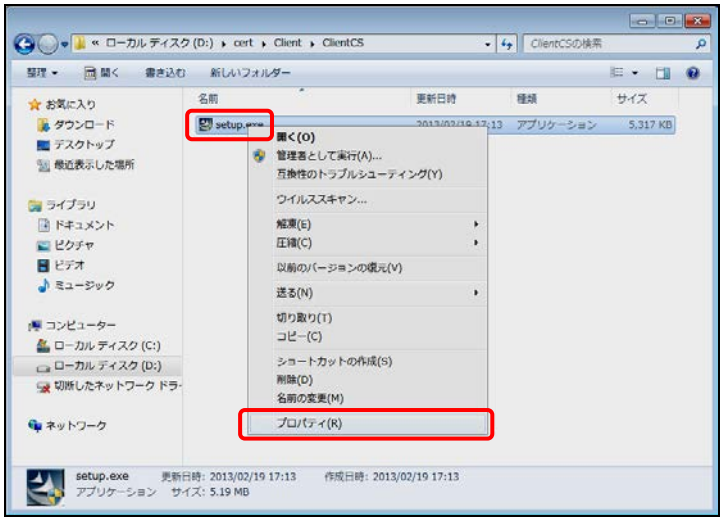
（2） セットアップファイルの署名の確認

セットアップを実行するファイル（setup 又は setup.exe）の発行元が正しいことを確認します。ClientCS 及び ClientUS のそれぞれの setup ファイルを確認してください。

1

「ClientCS」フォルダ又は「ClientUS」フォルダにある「setup.exe」ファイルを右クリックし、ショートカットメニューの《プロパティ》をクリックします。

※本項では、「ClientCS」フォルダの setup ファイルの署名を確認する手順のみを説明しています。「ClientUS」フォルダも同じ手順で確認してください。



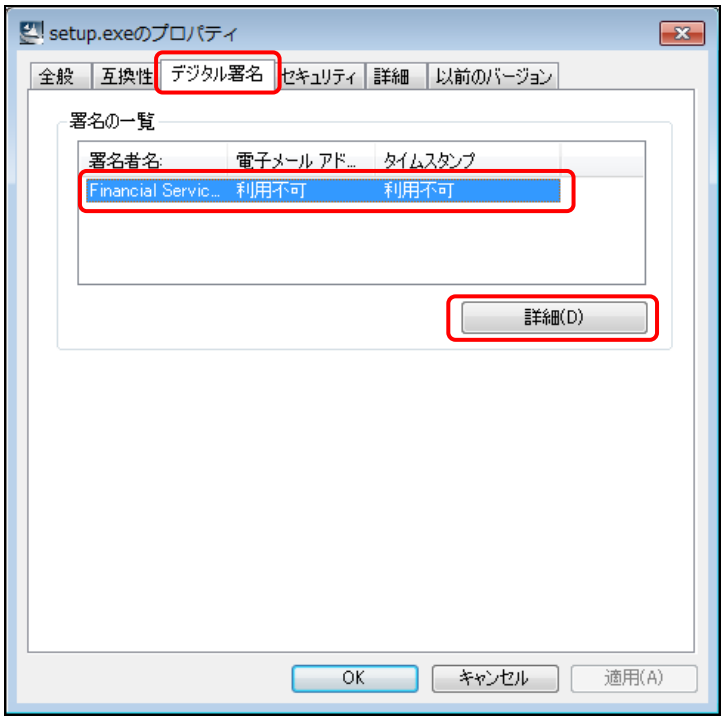
［setup.exe のプロパティ］が表示されます。

2

《デジタル署名》タブをクリックし、《署名の一覧》から署名をクリックします。

3

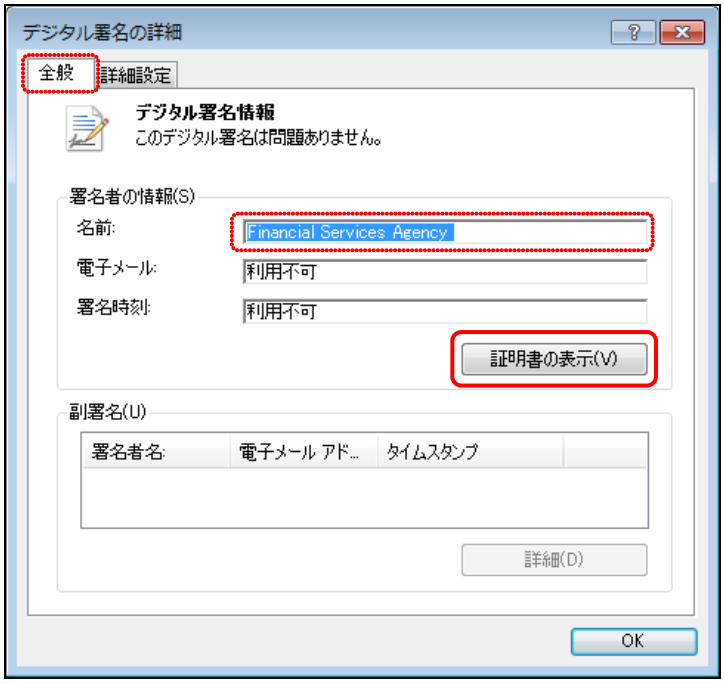
詳細(D)（詳細）をクリックします。



［デジタル署名の詳細］が表示されます。

4

《全般》タブを表示します。《署名者の情報》の《名前》が「Financial Services Agency」となっていることを確認し、証明書の表示(V)（証明書の表示）をクリックします。



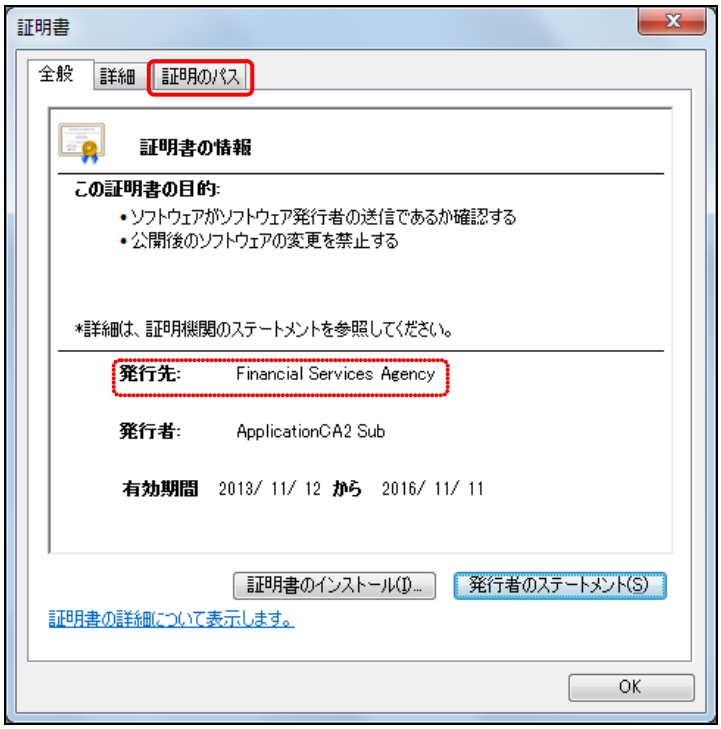
［証明書］が表示されます。

5

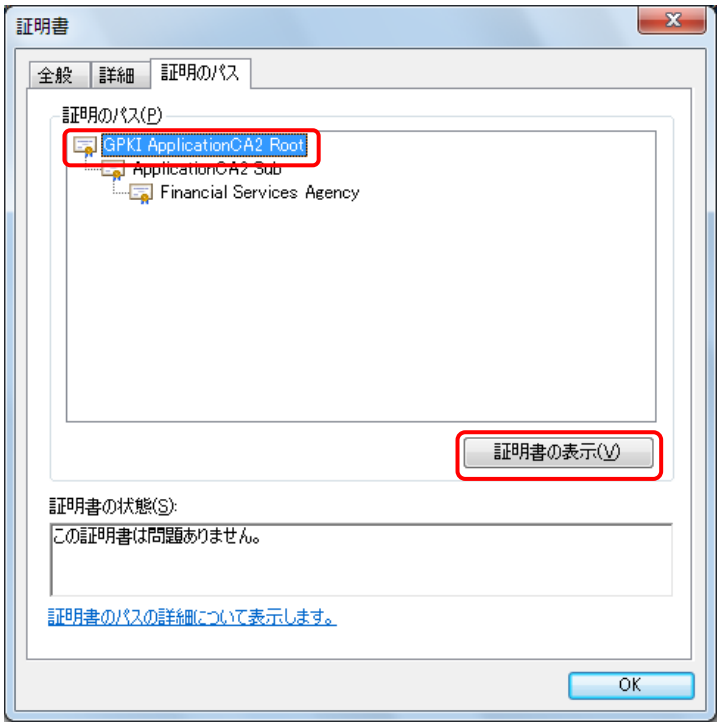
《全般》タブの「発行先」が「Financial Services Agency」となっていることを確認します。

6

《証明のパス》タブをクリックします。



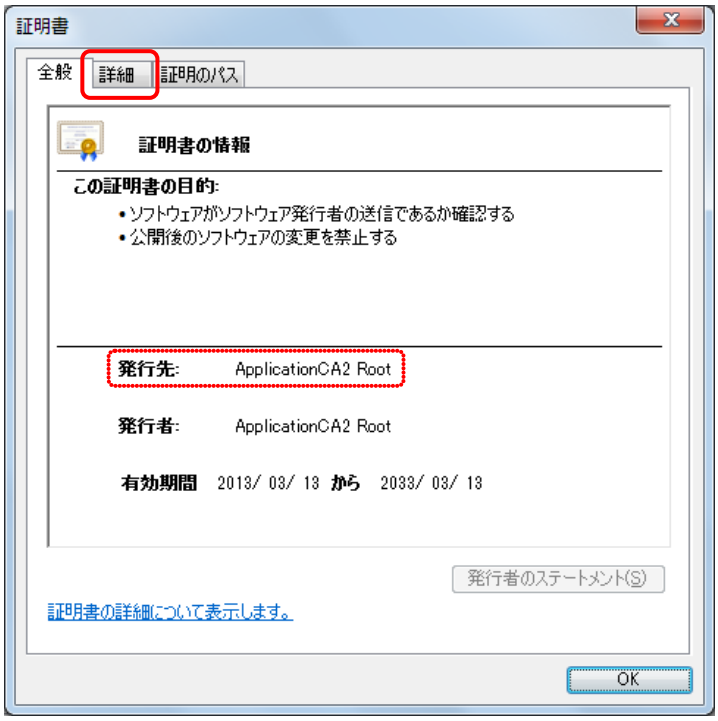
［証明のパス］タブが表示されます。



7

《証明のパス》の《GPKI ApplicationCA2 Root》を選択し 証明書の表示(V) （証明書の表示）をクリックします。

［証明書］が表示されます。



8

《全般》タブの《発行先》が「ApplicationCA2 Root」となっていることを確認します。

9

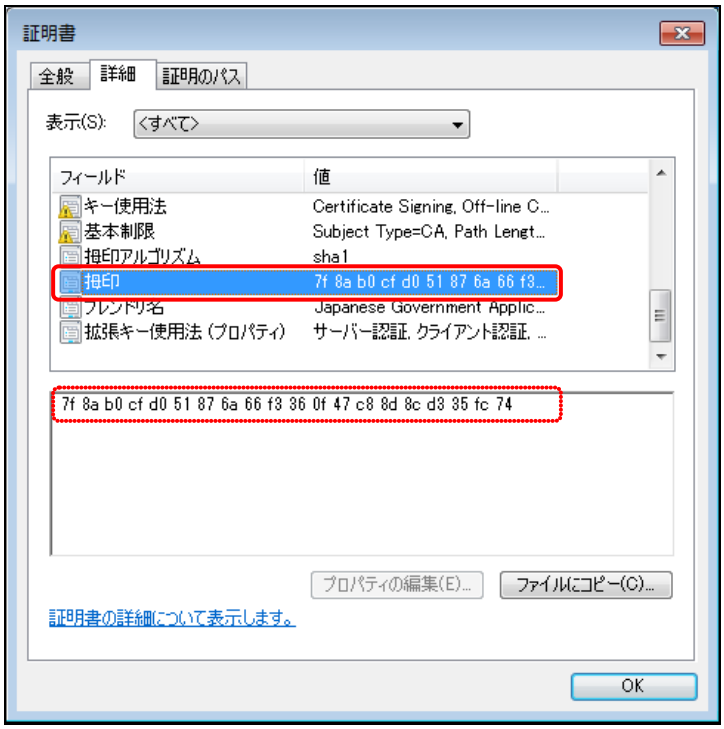
《詳細》タブをクリックします。

［詳細］タブが表示されます。

10

一覧から《拇印》をクリックします。
表示される拇印の内容を確認します。

操作 1 に戻り、同様の手順で「ClientUS」フォルダのセットアップファイルの署名も確認します。



(3) 署名機能クライアントのセットアップ

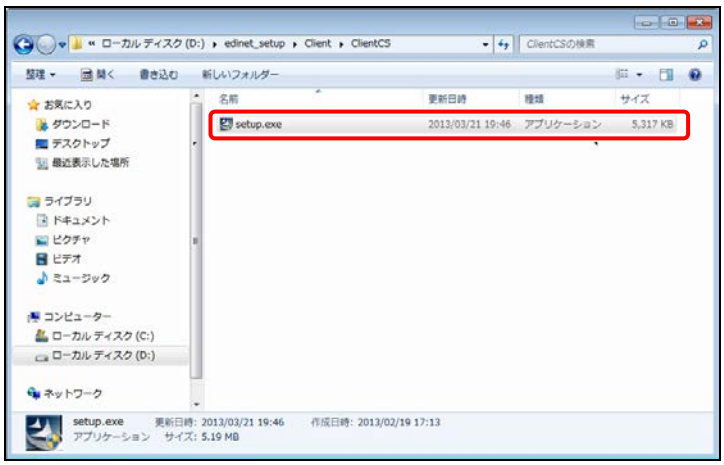
署名機能クライアントをセットアップします。

「ClientCS」フォルダのセットアップを実行後、「ClientUS」フォルダのセットアップを実行します。

1

「ClientCS」フォルダの「setup.exe」をダブルクリックします。

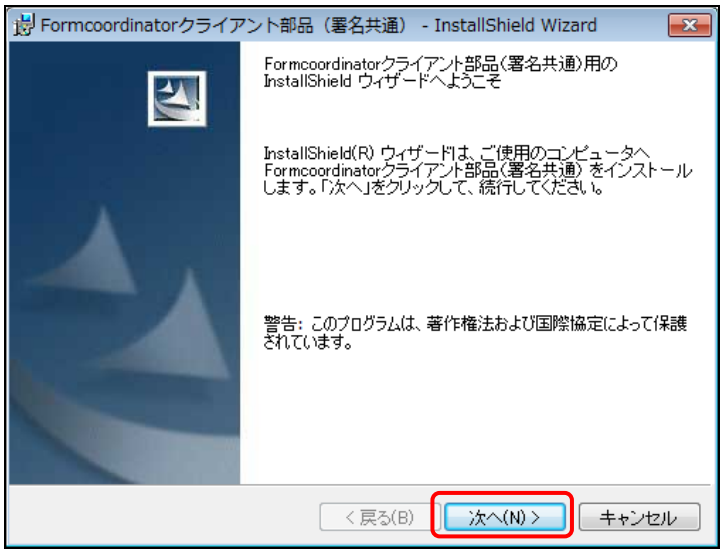
※本項では、「ClientCS」フォルダの setup ファイルのセットアップ手順のみを説明しています。「ClientUS」フォルダも同じ手順でセットアップしてください。



拡張子の表示　POINT

Windows の設定が、ファイルの拡張子を表示する設定になっている場合は右の図のように「setup.exe」と表示され、ファイル名の後ろに拡張子「.exe」が表示されます。表示しない設定の場合「setup」と表示されます。

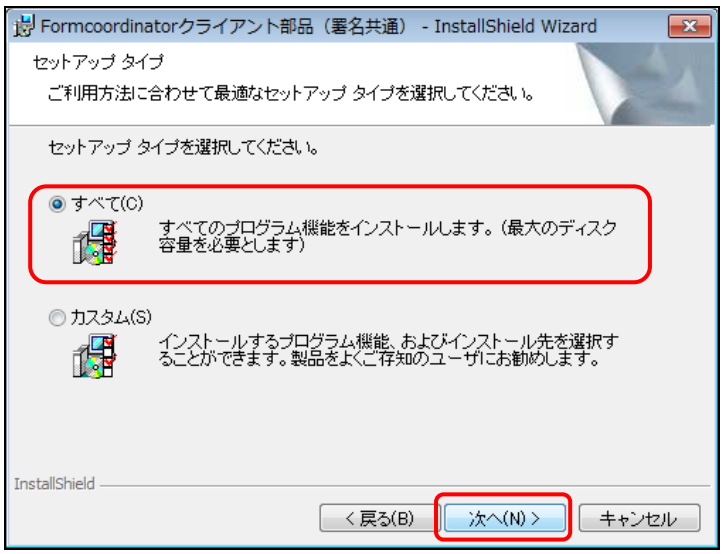
［Formcoordinator クライアント部品（署名共通） ウィザードへようこそ］が表示されます。



2

次へ(N) >（次へ）をクリックします。

［Formcoordinator クライアント部品（署名共通） セットアップタイプ］が表示されます。

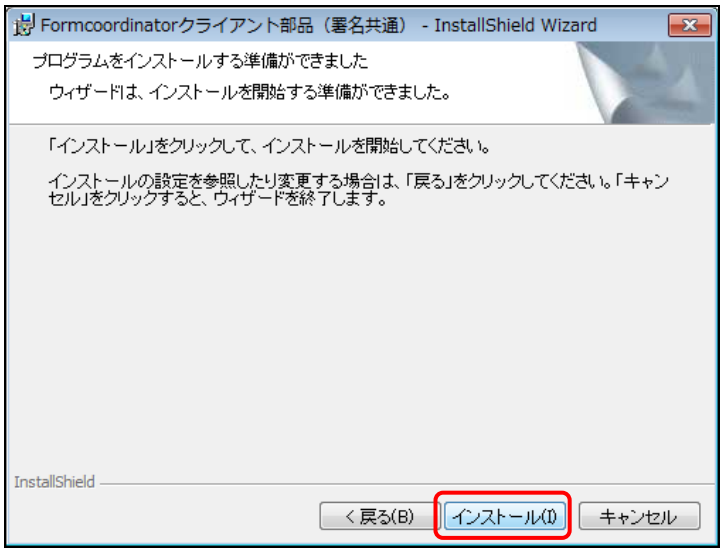


3

《セットアップタイプ》は「すべて」を選択し、次へ(N) >（次へ）をクリックします。

カスタム POINT

インストール機能又はインストール先を指定できます。

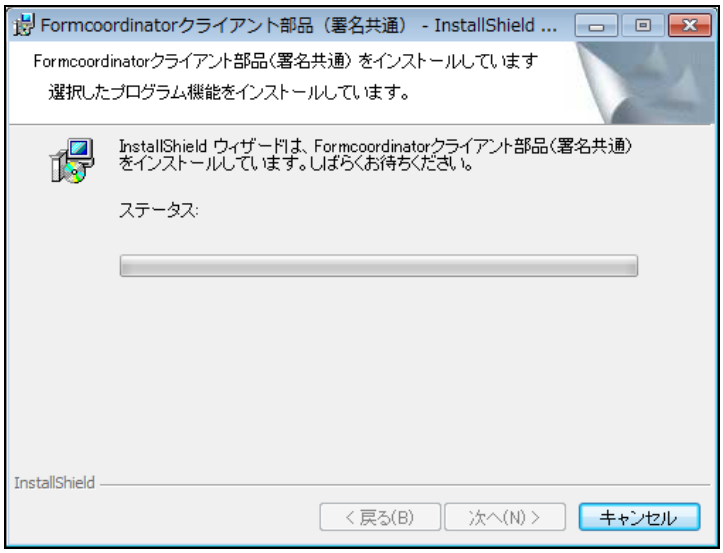


4

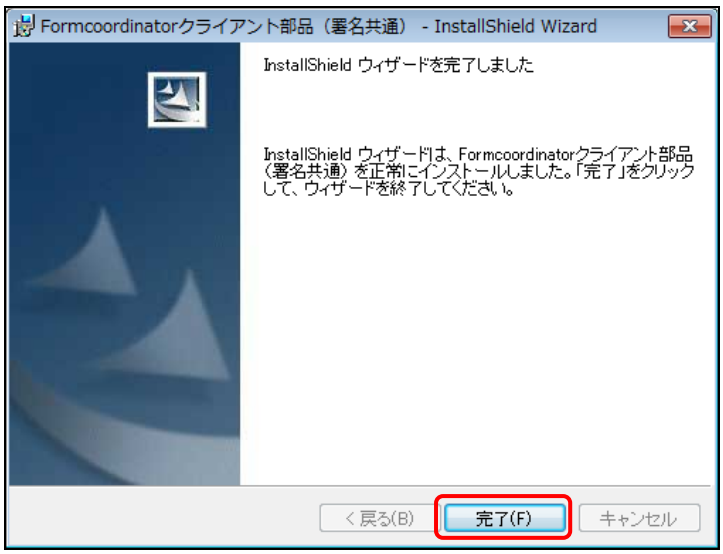
インストールを開始します。

インストール(I)（インストール）をクリックします。

インストールが開始されます。



インストールが完了すると、「**ウィザードを完了しました**」とメッセージが表示されます。



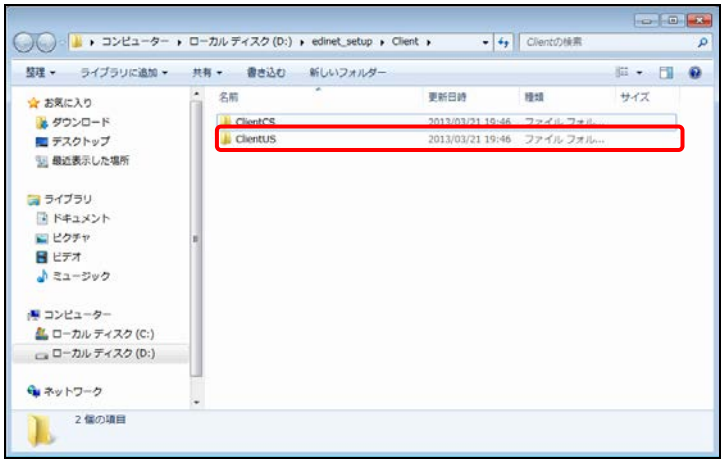
5

インストールを終了します。

完了(F) **(完了)をクリックします。**

署名機能クライアント（ClientCS）のセットアップが完了しました。

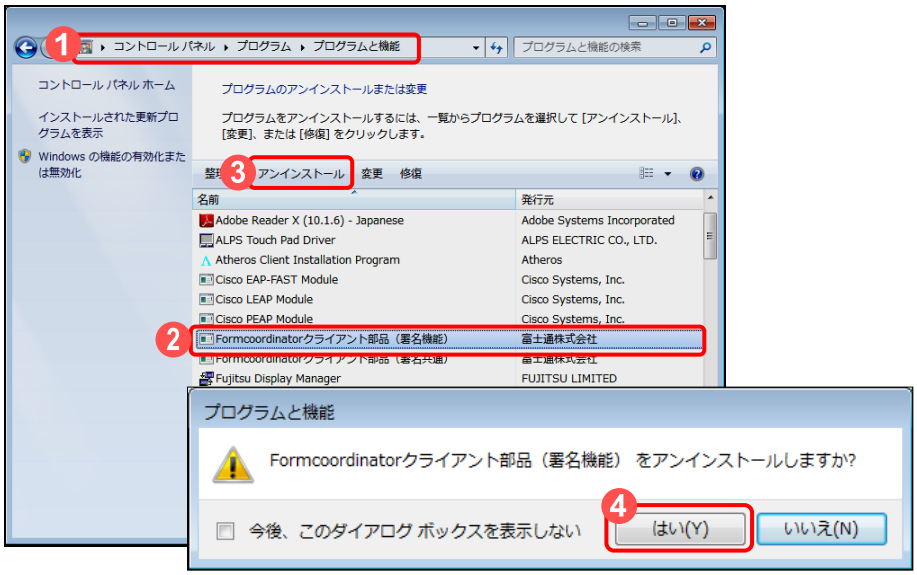
操作 1 に戻り、同様の手順で、「ClientUS」をセットアップします。



アンインストール

署名機能クライアントソフトが不要になった場合は、アンインストールします。

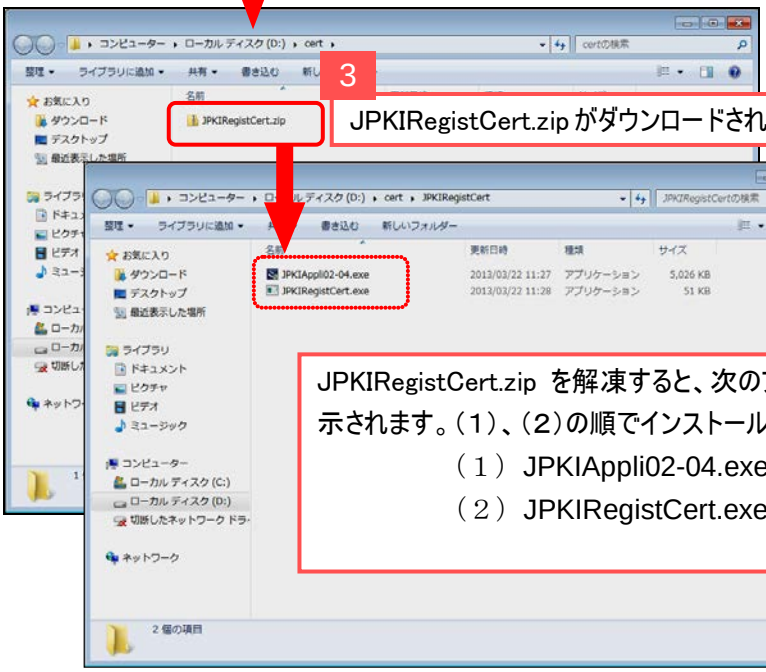
コントロールパネルの「プログラムのインストールまたは変更」から「Formcoordinator クライアント部品（署名機能）」を選択し、アンインストールします。



3-2-3 公的個人認証証明書登録ツールのセットアップ

EDINET からダウンロードした「**公的個人認証証明書登録ツール**」をセットアップします。

「**公的個人認証証明書登録ツール**」は、EDINET の［**開示書類等提出者のサイト**］にある「**トップメニュー**」の「**推奨端末仕様**」をクリックし、ダウンロードします。



JPKIRegistCert.zip を解凍すると、次のファイルが表示されます。(1)、(2)の順でインストールします。

（１） JPKIAppli02-04.exe

（２） JPKIRegistCert.exe

セットアップの手順は次のとおりです。

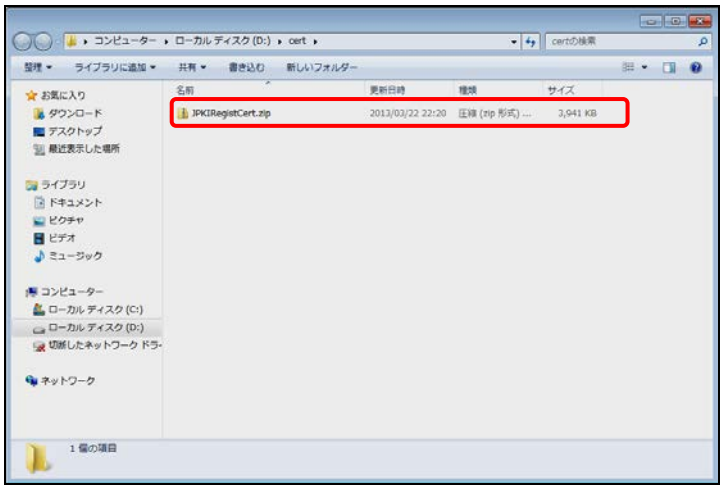
（1）ダウンロードした「JPKIRegistCert.zip」を解凍します。
（2）セットアップファイルの署名を確認します。
（3）「JPKIAppli02-04.exe」で利用者クライアントソフトをセットアップします。
（4）IC カードリーダを設定します。
（5）「JPKIRegistCert.exe」で IC カードの電子証明書を Web ブラウザに登録します。

（1） ダウンロードした「JPKIRegistCert.zip」の解凍

解凍ツールを利用する場合は、ツールの手順に従ってください。

1

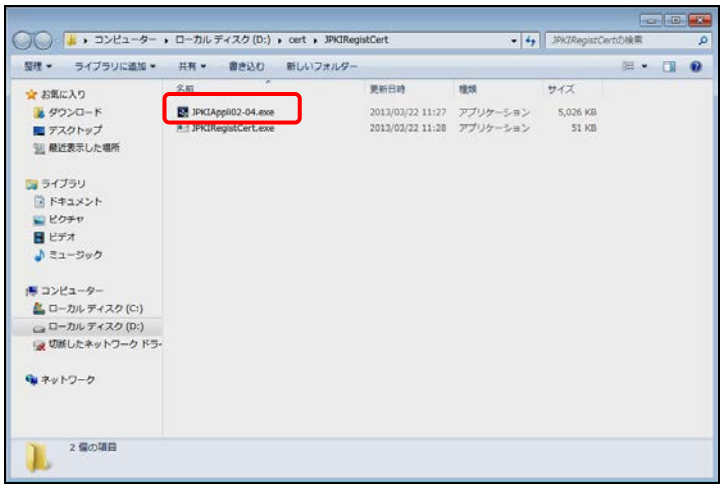
ダウンロードした「JPKIRegistCert.zip」を解凍します。



「JPKIAppli02-04.exe」及び「JPKIRegistCert.exe」の二つのファイルが作成されます。

2

「JPKIAppli02-04.exe」をダブルクリックします。



JPKIAppli02-04 及び JPKIRegistCert

POINT

両方をセットアップします。セットアップする順序は「JPKIAppli02-04」をセットアップ後、「JPKIRegistCert」をセットアップします。

拡張子の表示

POINT

Windows の設定が、ファイルの拡張子を表示する設定になっている場合は上の図のように「JPKIAppli02-04.exe」と表示され、ファイル名の後ろに拡張子「.exe」が表示されます。表示しない設定の場合「JPKIAppli02-04」と表示されます。

（2） セットアップファイルの署名の確認

セットアップを実行するファイル（JPKIAppli02-04 及び JPKIRegistCert）の発行元が正しいことを確認します。操作の手順は「**（2） セットアップファイルの署名の確認**」（p.18）を参照してください。

（3） 利用者クライアントソフトのセットアップ

利用者クライアントソフトをセットアップします。

利用者クライアントソフトのセットアップは、「**公的個人認証サービス ポータルサイト**（http://www.jpki.go.jp/index.html）」の「**利用者クライアントソフトのダウンロード**（http://www.jpki.go.jp/download/index.html）」を参照してください。

MEMO アンインストール

公的個人認証証明書登録ツールの利用者クライアントソフトが不要になった場合は、アンインストールします。

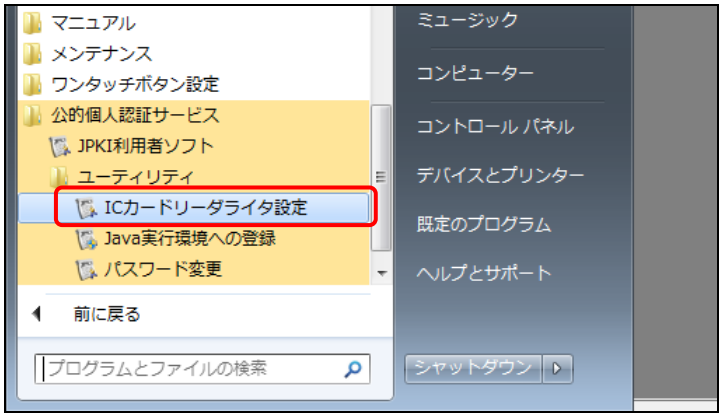
アンインストールの手順は、「利用者クライアントソフトのダウンロード（http://www.jpki.go.jp/download/index.html）」を参照してください。

（4） IC カードリーダの設定

利用者クライアントソフトで IC カードリーダを設定します。IC カードリーダをコンピュータに接続し、IC カードをセットします。

1

《スタート》から「公的個人認証サービス」の「ユーティリティ」の「IC カードリーダライタ設定」をクリックします。



[IC カードリーダライタ設定]が表示されます。

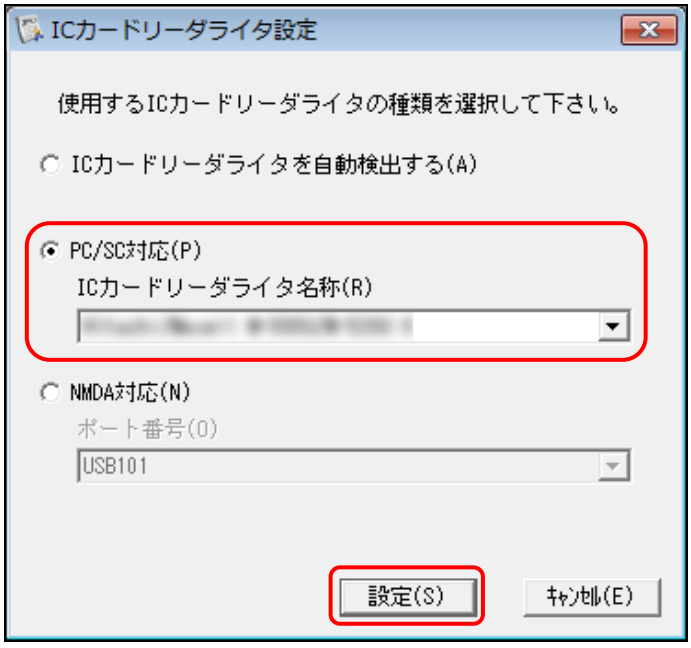
2

使用する IC カードリーダライタの種類を選択します。

※ここでは USB 経由で接続する IC カードリーダライタを選択します。

3

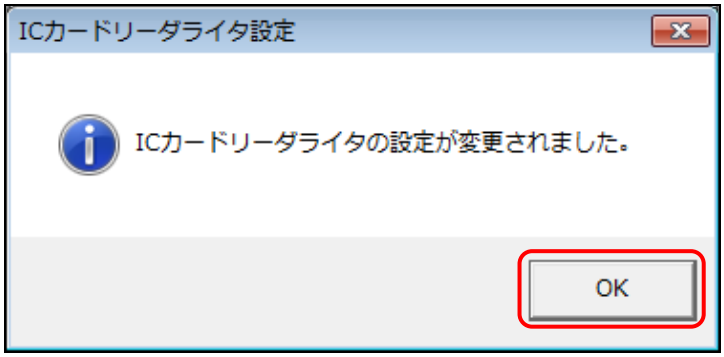
設定(S)（設定）をクリックします。



確認メッセージが表示されます。

4

OK（OK）をクリックします。

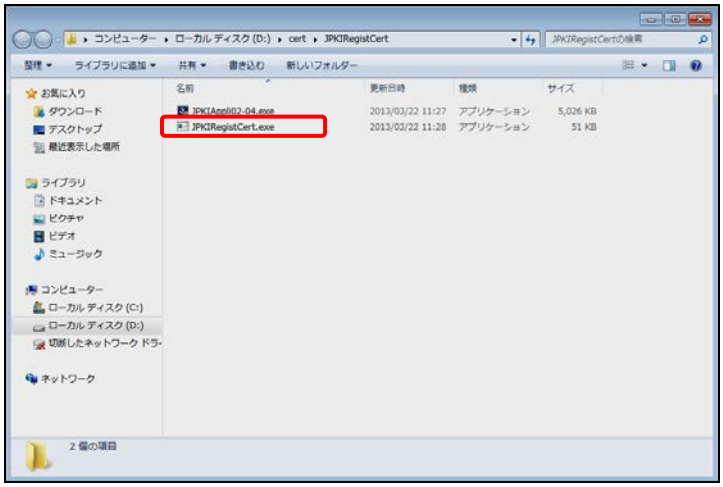


（5） IC カードの電子証明書を Web ブラウザに登録

パソコンと接続した IC カードリーダに IC カードを挿入し、IC カードに登録されている電子証明書を Web ブラウザに登録します。「（1） **ダウンロードした「JPKIRegistCert.zip」の解凍**」（p.26）でダウンロードした「JPKIRegistCert」ファイルを使用して登録をします。

1

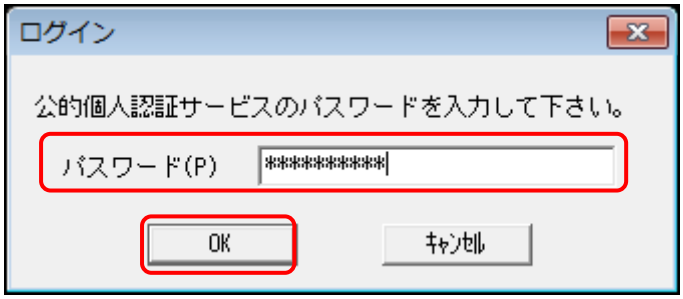
IC カードリーダに IC カードが挿入されていること及びパソコンに接続されていることを確認します。



2

「JPKIRegistCert.exe」をダブルクリックします。

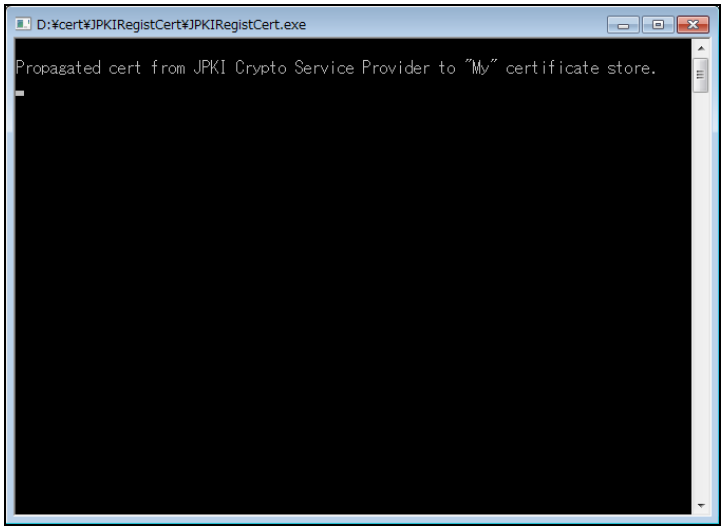
［**ログイン**］が表示されます。



3

IC カードの《パスワード》を入力し、 OK **(OK)をクリックします。**

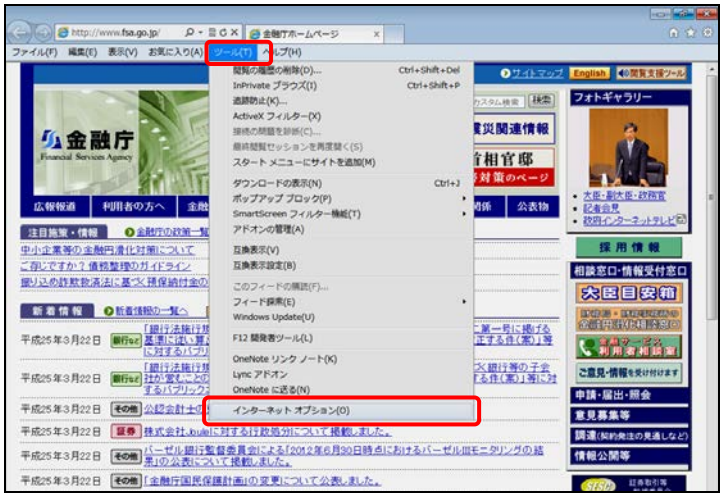
メッセージ画面が表示され、自動的に閉じられます。



証明書が Web ブラウザに登録されたことを確認します。

4

Web ブラウザを起動し、メニューバーの《ツール》から《インターネット　オプション》をクリックします。



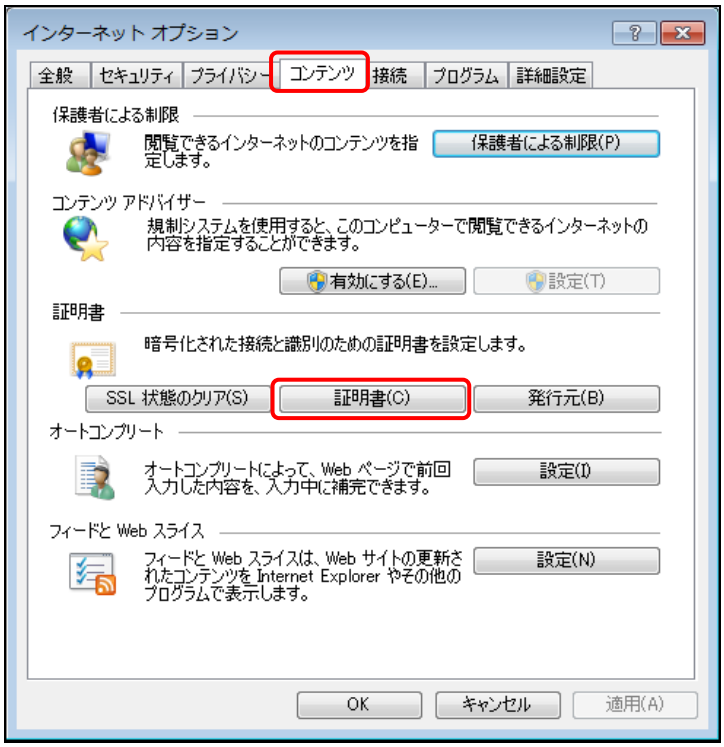
［インターネット　オプション］が表示されます。

5

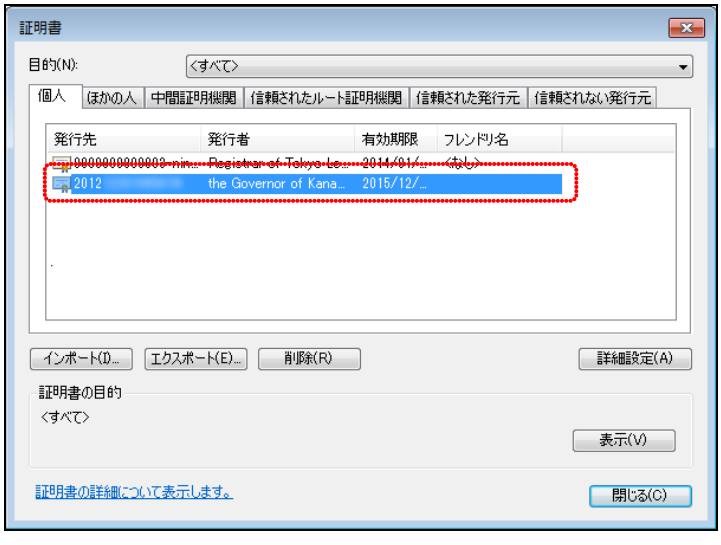
《コンテンツ》タブをクリックします。

6

証明書(C)（証明書）をクリックします。



［証明書］が表示されます。
IC カードの電子証明書が一覧に追加されていることを確認します。



3-3 商業登記

EDINET に書類提出する際に、商業登記の署名を付与して提出する場合の事前準備について説明します。

3-3-1 事前準備

電子証明書を事前に入手してください。
既に入手済みの方は、証明書の期限切れ、失効等がないか、確認してください。
※証明書が期限切れ、失効等している場合、書類に署名を付与する操作の際にエラーとなります。

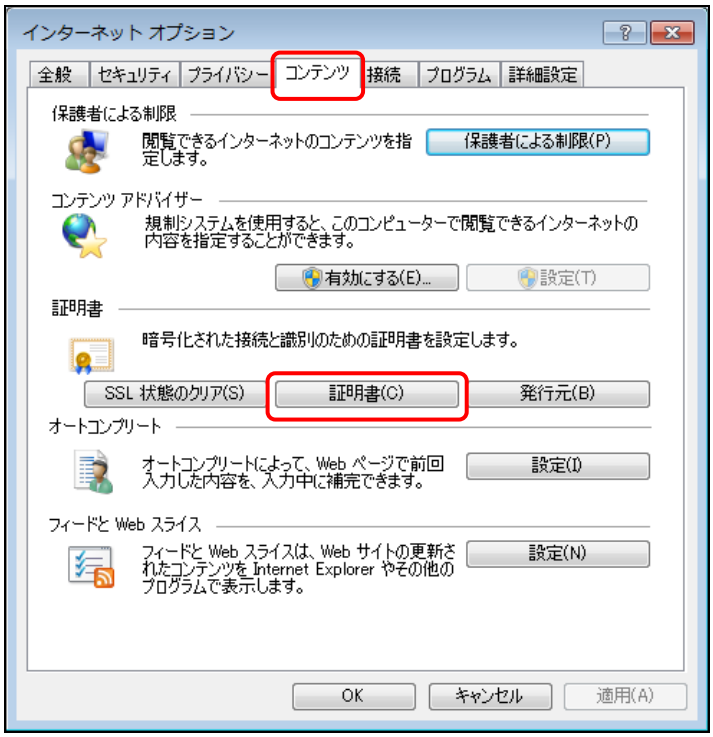
3-3-2 証明書の登録

証明書を Web ブラウザに登録します。

1

メニューバーの《ツール》から《インターネット　オプション》をクリックします。

[インターネット オプション]が表示されます。



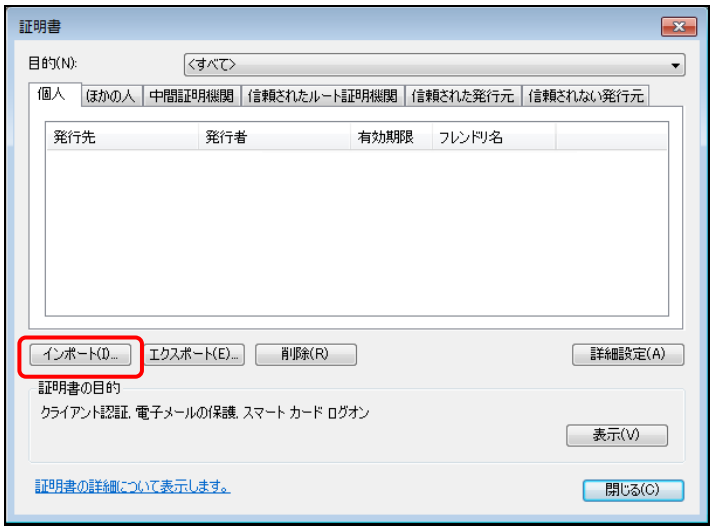
2

《コンテンツ》タブをクリックします。

3

証明書(C)（証明書）をクリックします。

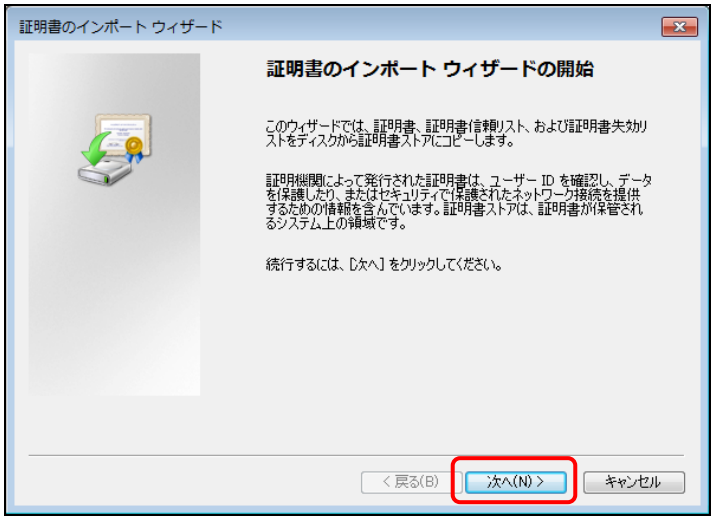
[証明書]が表示されます。



4

インポート(I)...（インポート）をクリックします。

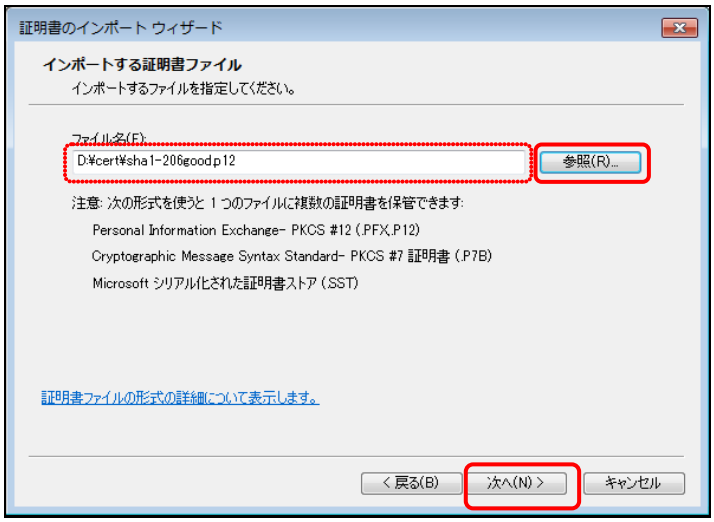
[証明書のインポート ウィザード]が表示されます。



5

次へ(N) >（次へ）をクリックします。

［インポートする証明書ファイル］が表示されます。



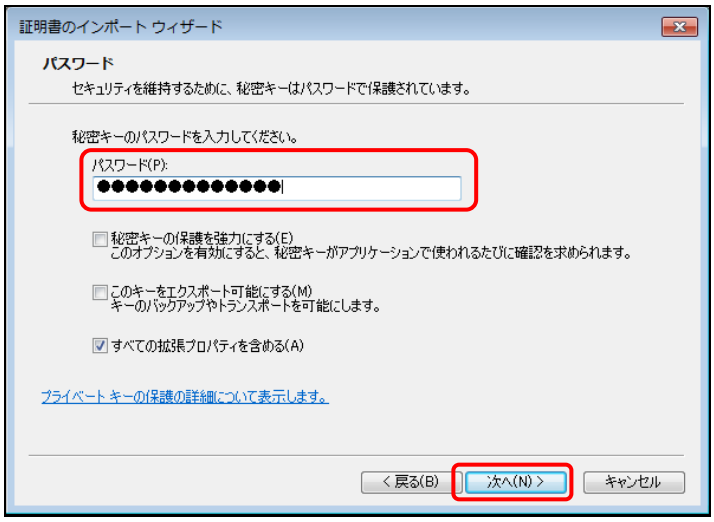
6

参照(R)...（参照）をクリックし、Web ブラウザに登録する証明書の保存先を指定します。

7

次へ(N) >（次へ）をクリックします。

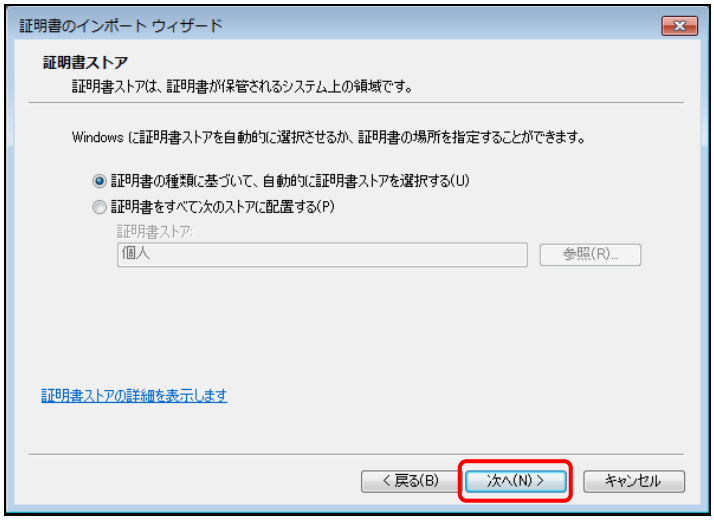
［パスワード］が表示されます。
※表示されない場合は操作 9 に進みます。



8

証明書のパスワードの指定が必要な場合は、パスワード入力画面が表示されます。《パスワード》を入力し、次へ(N) >（次へ）をクリックします。

［証明書ストア］が表示されます。



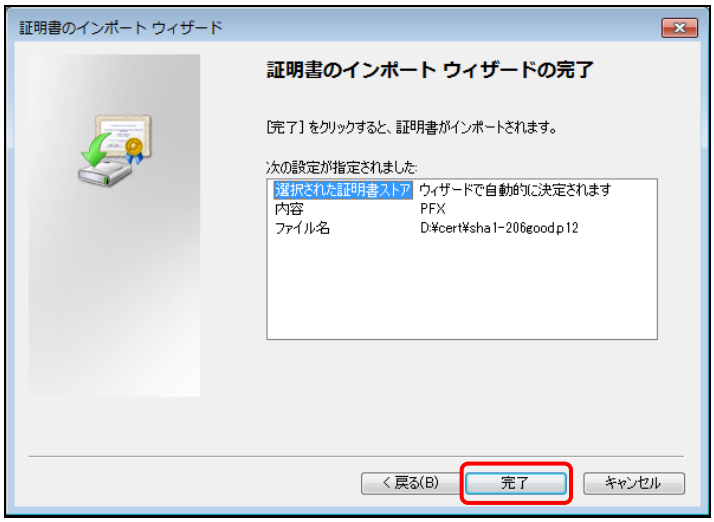
9

証明書を配置するストアを指定し、次へ(N) >（次へ）をクリックします。

配置するストア　POINT

指定がなければ、既定のまま操作を続けてください。

［証明書のインポートウィザードの完了］が表示されます。

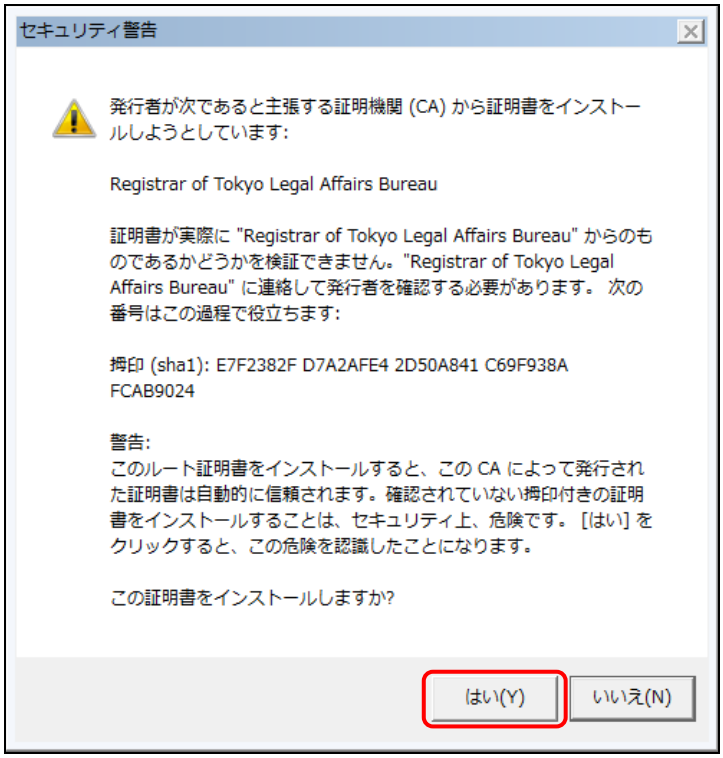


10

証明書のインポートが完了します。

完了 (完了)をクリックします。

［セキュリティ警告］が表示されます。



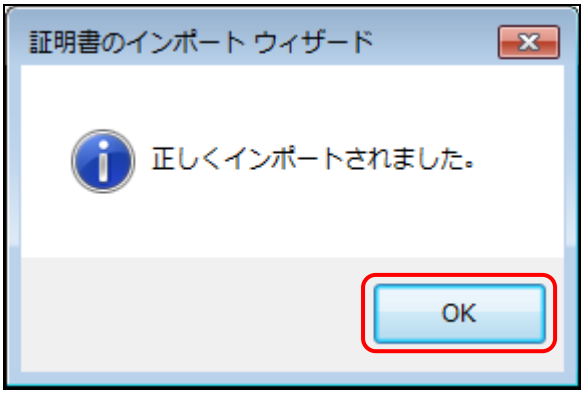
11

内容を確認し、はい(Y) (はい)をクリックします。

ルート証明書のインストール　POINT

電子証明書発行者の証明機関からルート証明書がインストール済みの場合は、本メッセージは表示されません。
操作 12 に進んでください。本メッセージが表示された場合は、本メッセージ内にある拇印をメモし、操作 13 以降の手順で拇印を確認してください。

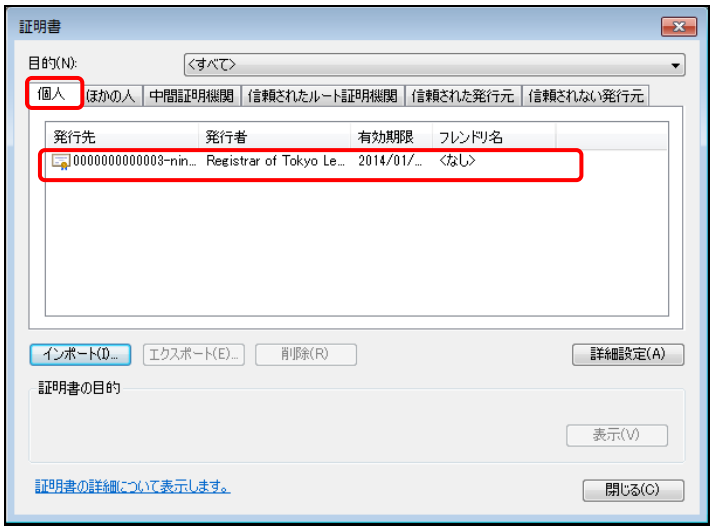
確認メッセージが表示されます。



12

OK (OK)をクリックします。

［証明書］が表示されます。



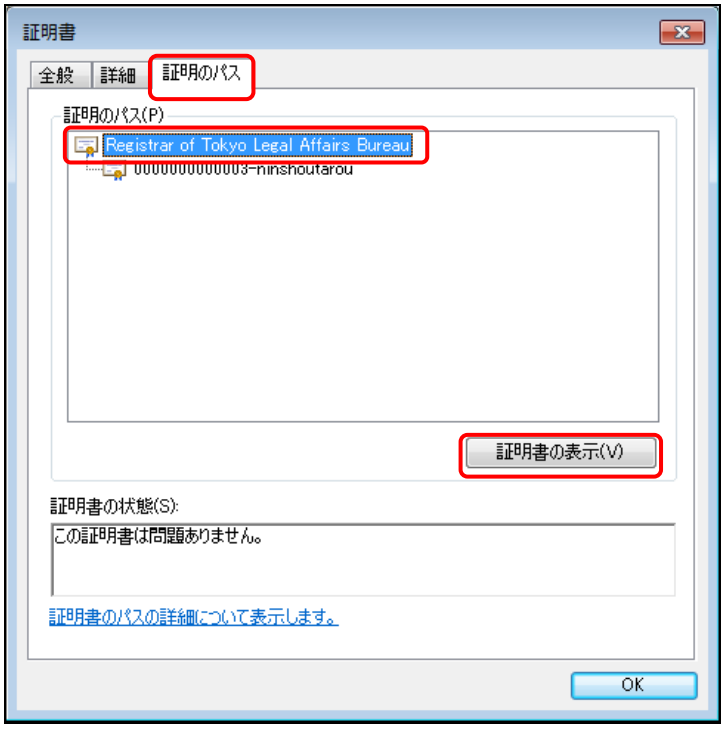
13

《個人》タブをクリックし、一覧に証明書が登録されていることを確認します。

14

証明書の内容を確認します。証明書名をダブルクリックします。

［証明書］が表示されます。



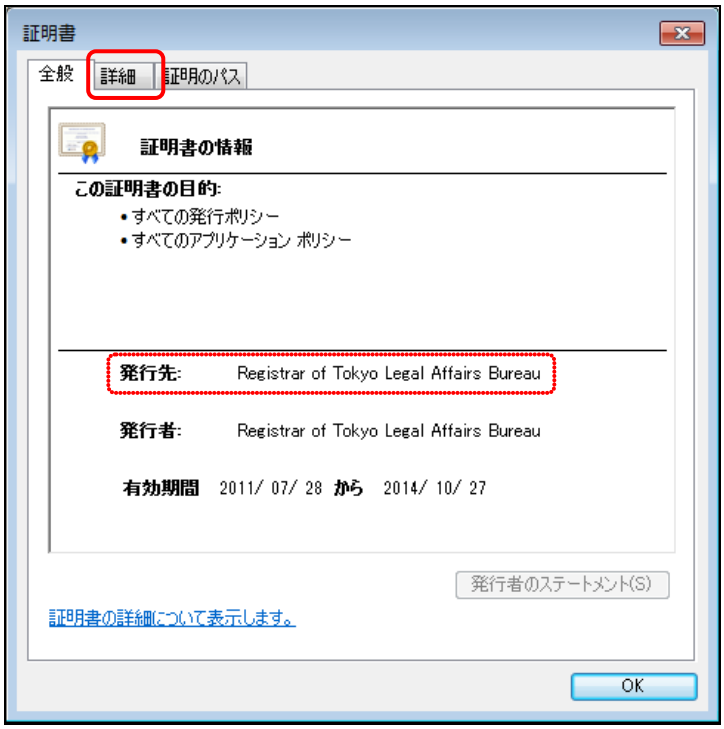
15

《証明書のパス》タブをクリックします。

16

《証明書のパス》のルート証明書をクリックし、証明書の表示(V)（証明書の表示）をクリックします。

［証明書］が表示されます。



17

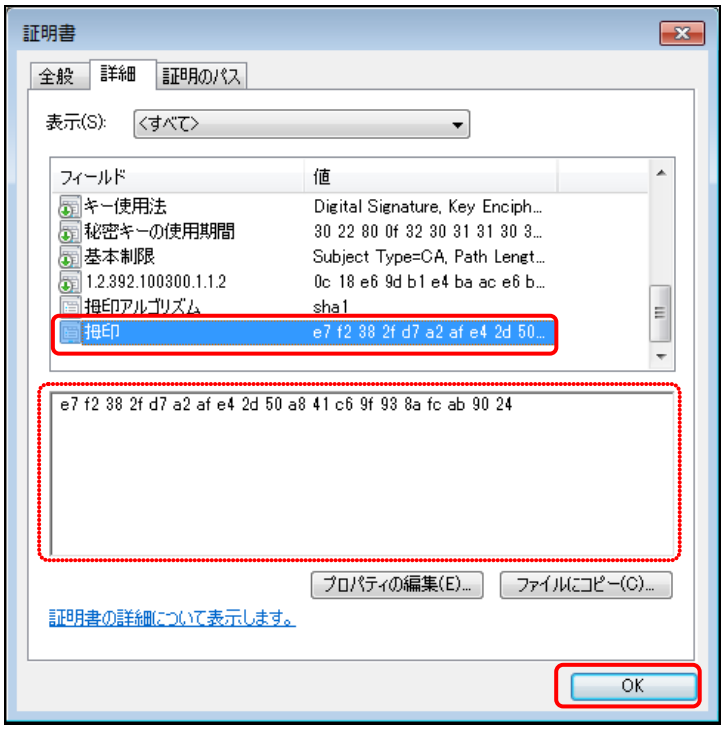
《全般》タブの《発行先》を確認します。

18

《詳細》タブをクリックします。

19

一覧から《拇印》をクリックします。
表示される拇印の内容を確認します。



20

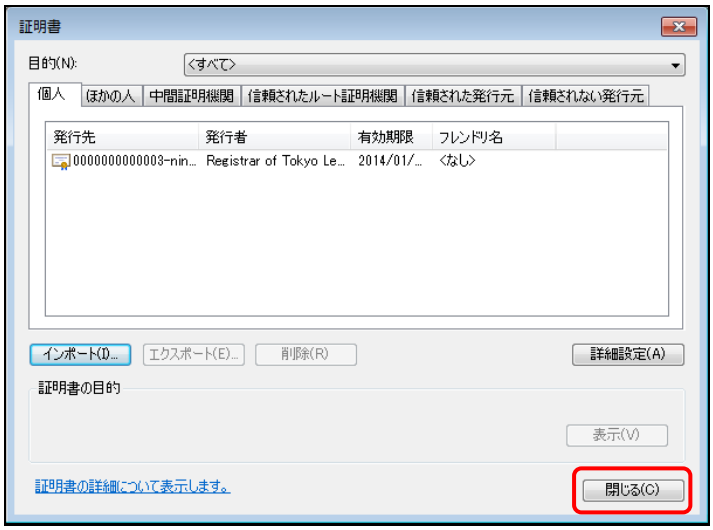
確認を終了します。

OK (OK)をクリックします。

21

設定を終了します。

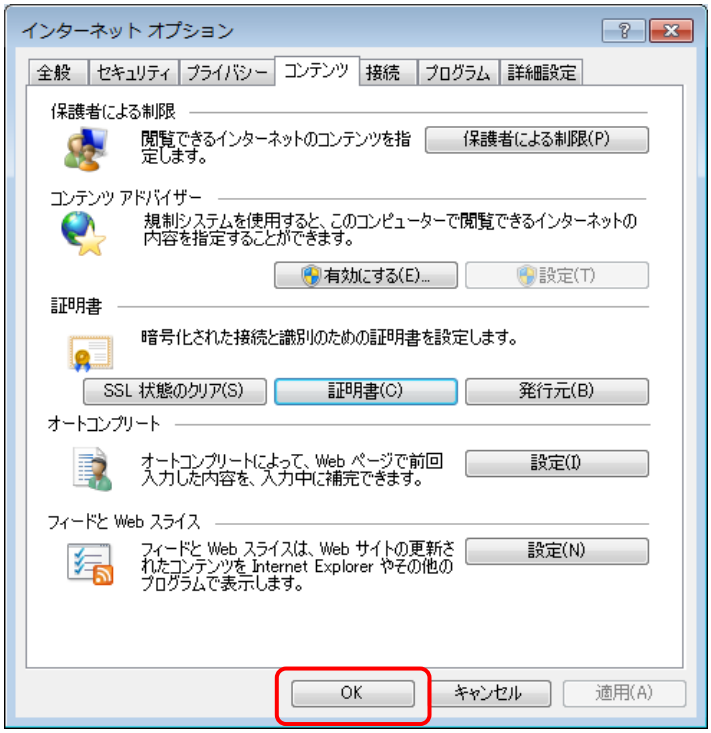
閉じる(C)（閉じる）をクリックします。



［**インターネット　オプション**］が表示されます。

22

OK（OK）をクリックします。



証明書が登録されました。

■■■ 改版履歴 ■■■

No.	改版日	改版内容
1	2013.08	初版
2	2013.09	「2-3-1 証明書設定の必要性確認」の「MEMO[セキュリティの警告]が表示されない場合」について、「《発行者》が「ApplicationCA」と表示されることを確認します。」へ変更。
3	2013.12	「2-3-1 証明書設定の必要性確認」の「MEMO[セキュリティの警告]が表示されない場合」について、《発行者》を「ApplicationCA2 Sub」へ変更。 「3-2-2 署名機能クライアントのセットアップ」の「7」について、「《証明のパス》の《GPKI ApplicationCA2 Root》を選択し」へ変更。 「3-2-2 署名機能クライアントのセットアップ」の「8」について、「《全般》タブの《発行先》が「ApplicationCA2 Root」となっていることを確認します。」へ変更。 「3-2-2 署名機能クライアントのセットアップ」の画像について、証明書変更のため、差し換え。 政府認証基盤（GPKI） の認証の更新のため、「アプリケーション認証局の自己署名証明書」を「アプリケーション認証局2(Root)の自己署名証明書」へ変更。あわせて、「2-3-2 証明書の設定」の画像を差し替え。 「2-3-2 証明書の設定」の「2」について、「《アプリケーション認証局2》をクリックし、」へ変更。
4	2014.04	「1 操作環境について」の「＜ソフトウェア＞」について、オペレーティングシステム「WindowsXP」を削除し、「Windows8」及び「Windows8.1」を追加。 Web ブラウザに「Internet Explorer 10」及び「Internet Explorer 11」を追加。 JRE を「Version7 Update7」から「Version7 Update51」に変更。
5	2015.02	「1 操作環境について」に JRE8 を追加。 「1 操作環境について」の「＜ソフトウェア＞」について、JRE を「Version7 Update51」から「Version7 Update75」に変更し、「Version8 Update31」を追加。
6	2015.03	「3-1 電子証明書について」の「民間認証局の一覧」を更新。
7	2015.04	「1 操作環境について」から JRE7 を削除。 「1 操作環境について」の「＜ソフトウェア＞」について、JRE を「Version8 Update31」を「Version8 Update45」に変更し、「Version7 Update75」を削除。

EDINET Electronic Disclosure for Investors' NETwork

書類提出用 端末要件

平成 27 年4月　　1.6 版